

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-160490

(43)Date of publication of application : 20.06.1997

(51)Int.Cl.

G09C 1/00

H03M 7/30

H04L 9/22

(21)Application number : 07-344385

(71)Applicant : KO SHINU

(22)Date of filing : 06.12.1995

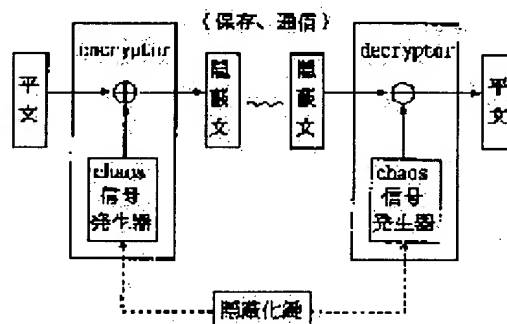
(72)Inventor : KO SHINU

(54) METHOD AND APPARATUS FOR CONCEALING AND DECODING INFORMATION BY DIGITAL TYPE CHAOS SIGNAL

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a novel concealing and decoding system capable of dealing with a request for safe and high-speed communication.

SOLUTION: The plain text information is concealed by applying the digital type chaos signal vectors generated in accordance with (1) a chaos function, (2) initial value, (3) delay and (4) parameters of the chaos function determined by the keys of variable length composed of the character string of an arbitrary length assigned for each of the signal units of the plain text information. The information is decoded by using the chaos signal vectors formed by the same key as the key at the time of the concealing for each of the signal units of the concealed signals.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-160490

(43) 公開日 平成9年(1997)6月20日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 1 0	7259-5J	G 0 9 C 1/00	6 1 0 D
H 0 3 M 7/30		9382-5K	H 0 3 M 7/30	B
H 0 4 L 9/22			H 0 4 L 9/00	6 5 5

審査請求 未請求 請求項の数4 F D (全 7 頁)

(21) 出願番号 特願平7-344385

(22) 出願日 平成7年(1995)12月6日

(71) 出願人 593221598

高 振宇

埼玉県川口市金山町1番4-205号シャトープリンス

(72) 発明者 高 振宇

埼玉県川口市金山町1番4-205号シャトープリンス

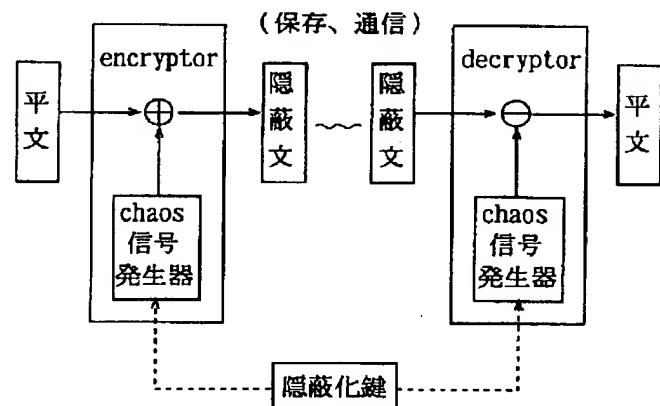
(74) 代理人 弁理士 豊田 正雄

(54) 【発明の名称】 デジタル式カオス信号による情報の隠蔽・復号化方法および装置

(57) 【要約】

【課題】 安全で高速通信の要求に対応できる新たな隠蔽化・復号化方式をえる。

【解決手段】 平文情報の信号単位ごとに、指定された任意長の文字列により構成された可変長の鍵によって決めた(1)カオス(chaos)関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで平文情報を隠蔽化し、該隠蔽化された信号の信号単位ごとに隠蔽化時と同一の鍵により生成したカオス信号ベクトルを用いて復号する。



【特許請求の範囲】

【請求項1】 平文情報の信号単位ごとに、指定された任意長の文字列により構成された可変長の鍵によって決めた(1)カオス(chaos)関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで前記平文情報を隠蔽化し、前記隠蔽化された信号の信号単位ごとに隠蔽化時と同一の鍵により生成したカオス信号ベクトルと平文情報の信号を用いて復号することを特徴とする隠蔽・復号化方法。

【請求項2】 平文情報の信号単位ごとに、指定された任意長の文字列により構成された可変長の鍵によって決めた(1)カオス(chaos)関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで前記平文情報を隠蔽化する方法を直列多段階行って隠蔽化し、該隠蔽化された信号の信号単位ごとに各段の隠蔽化時と同一の鍵により生成したカオス信号ベクトルを用いて直列多段階行って復号することを特徴とする隠蔽・復号化方法。

【請求項3】 平文情報の信号単位ごとに、指定された任意長の文字列により構成された可変長の鍵によって決めた(1)カオス(chaos)関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで、平文情報を変換する隠蔽化手段を備えたことを特徴とする信号隠蔽化装置。

【請求項4】 平文情報の信号単位ごとに、指定された任意長の文字列により構成された可変長の鍵によって決めた(1)カオス(chaos)関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで、平文情報を変換して隠蔽化された信号の信号単位ごとに隠蔽化時と同一の鍵により生成したカオス信号ベクトルを用いて復号する信号復号手段を備えたことを特徴とする復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はコンピュータ通信システムの情報機密保護のために行われるデジタル式カオス信号による隠蔽・復号化方法および装置に関する。

【0002】 コンピュータ通信システムの隠蔽・復号化方式は、情報、データなどのデジタル信号を保存、伝送、通信する際に、その機密保護、偽造や改ざんを防止するための情報処理技術である。現在では、電子通信からコンピュータ・ネットワーク、銀行、企業、特に来世紀のエレクトロニック・コマスを実現するための各種電子決済システムまで、非常に広い範囲で使われており、情報社会に不可欠な技術となっている。

【0003】

【従来の技術】 コンピュータデータの機密保護のための方式としては、1977年米商務省標準局に採用されたDE

S(Data Encryption Standard)に代表される一般的な方式と、Rivest、Shamir、Adelmanの3人による開発されたRSA方式に代表されるPublic Key Cryptography方式に分類される。

【0004】 その一方、各種の情報機密保護方式が開発されると同時に、対応する解読法(cryptanalysis)の研究も進んでいる。例えば、アメリカのA. Shamirが日本のNTTのFEAL-8という機密保護方式によって作成されたデータを解読した例もある。即ち、機密保護の安全性は時間とともに劣化していくものである。

【0005】

【発明が解決しようとする課題】 従来のコンピュータデータの隠蔽・復号化システムの問題点を以下に指摘する。

(1) アルゴリズムは容易に更新できない。

(2) 固定長の鍵：可変長の鍵の場合より有限な時間内に鍵を割り出すやすい。また、便利さと安全さのバランスをユーザが自由に選択できない。

(3) ブロック型のものなら、そのアルゴリズムは計算循環周期性があるので、画像データ、音声データのような同様な信号パターンが連続的に出現するファイルを隠蔽化する場合、解読できるので、マルチメディア時代に適用できない。

(4) ブロック的な処理ではアルゴリズムは複雑過ぎるので、処理速度が遅くなり、高速通信に対応できない。

(5) DESとRSAともに十数年前に開発されたものであるため、古くなり、それらの安全性はすでに保証できなくなり、それらの寿命は今世紀末までである。

【0006】 本発明は、これらの従来の隠蔽・復号化方式の欠点を除き、より安全かつより高速な新たな隠蔽・復号化方法および装置を開発することを目的とする。

【0007】

【課題を解決するための手段】 上記目的を達成するために本発明は、「初期値に敏感に依存する」、「予測不可能」などの特性を有するデジタル式のカオス信号(chaos)を利用することで、上述した問題を解決する。即ち、平文情報の信号単位ごとに、指定された任意長の文字列により構成された鍵によって決めた(1)カオス関数、(2)初期値、(3)遅れ、(4)カオス関数のパラメータに基づいて、発生したデジタル式カオス信号ベクトルを付加することで前記平文情報を隠蔽化し、該隠蔽化された信号の信号単位ごとに隠蔽化時と同一の鍵により生成したカオス信号ベクトルを用いて復号する隠蔽・復号化方式である。

【0008】 本発明の手順を図1に示す。使用者の指定された鍵とデジタル信号からなる平文(元の情報)を本システムに伝送して、本システムの内部ではその鍵によって発生されたカオス信号を平文に文字単位でストリームに付加することで、隠蔽化信号文を得る。復号するとき、同様な鍵と隠蔽化信号文を本システムに伝送すれ

ば、同様の原理で平文を得られる。

【0009】カオス(Chaos)は混沌を意味するギリシャ語であり、空気の流れの乱流のように不規則、予測不可能に見える現象である。アメリカのHermann Hakenは「決定論的方程式から生じる不規則運動のことをカオスという」と定義している。従来の確定論と確率論間の垣根を取り外すものと思われるカオスは、現在、人類の残った科学難題や未明現象を解明するための最先端の科学理論として科学や工学などの諸分野に大きな影響を及ぼしている。ランダム現象とは違い、簡単な規則の下での複雑さといえる。「初期値に敏感に依存する」、「予測不可能」、「一刻でも停止しない」などの特性を有する。図2はロジスティック写像と呼ばれるカオス関数の時系列波形を示すグラフである。

【0010】本発明の原理について説明する。入力データとなる平文を $P(i)$ 、信号文を $C(i)$ 、鍵を $K(j)$ 、カオス信号を $Chv(i)$ とする。

【0011】 $P()$ と $C()$ をバイト単位で処理するもの、その長さは n バイトとして、 $K()$ をアスキーコードからなる文字列(例えば、 $a \sim z, 0 \sim 9$)、その長さは m とする。即ち、

$$0 < i \leq n, 0 < j \leq m$$

とする。本発明の隠蔽化手続きを図3に、復号化手続きを図4に示す。

【0012】デジタルカオス信号発生関数 $Chv()$ については、各種のカオス関数で入れ替えることが可能である。例えば、ロジスティック写像と呼ばれるカオス関数を次のように定義できる。

```
Ch1(n, p) begin  $X_{n+1} = p * X_n (1.0 - X_n)$  return  $(X_{n+1})$  end
```

【0013】また、繰り返し公式によるカオス関数ならば次のように定義できる。

```
Ch2(n, p) begin  $X_{n+1} = X_n^2 - p$  return  $((X_{n+1} + 2.0) / 4.0)$  end
```

【0014】キー処理モジュールでは下記の $f()$ に示すように、ユーザの入力された任意長の文字列を暗号キー K としてレジスタに置き、この K を用い、準備しておく複数のカオス関数の中から使用しようとするカオス関数の番号 v を決め、また、そのカオス関数の初期値 $init$ 、カオス信号の遅れ $delay$ 、及びカオス関数のパラメータ p (複数も可能)を同時に決める。

【0015】 $f(K)$

```
begin
job = (double)(K)/L
init = job - (long int)(job)
delay = (long int)(job) mod B
p = delay/L - (long int)(delay/L)
v = (int)(delay/L) mod D
end
```

ただし、 L はある無理数(例えば、 $L = \pi$ などの値も用い

られる)、 D は準備しておくカオス関数の個数、 B は $> D$ の正整数である。

【0016】上述したアルゴリズムを基本部品とすれば、図5に示すように直列に利用することによって、多鍵多重カオスを用いたシステムを構成することもできる。これによって、いろいろな用途に対応でき、より安全なシステムとなる。

【0017】本発明の方式を用いることにより、現在使われている解読手法では、鍵が分らないとカオス隠蔽を解読することが不可能である。また、目的に合わせて、多鍵多重カオスを用いたシステムを採用すれば、より安全になる。さらにカオス関数は入れ換えることができるので隠蔽化処理のルールはいつでも更新できる。可変長鍵であるから、鍵の空間(組み合わせ個数)はより多くなる。

【0018】即ち、同様の n 桁 m 進数値の鍵には、

固定長鍵の場合: m^n

可変長鍵の場合:

【0019】

【数1】

$$m^n + \sum_{i=1}^{n-1} m^{n-i}$$

【0020】の組み合わせがある。カオス信号の発生は速く、かつ、ストリーミ的な処理であるから、信号の隠蔽化と復号の処理は、ブロック単位ではなく、信号のバイトつづにカオス信号を付加するというような信号単位でストリーミ的に行うから、連続的に送受信できる。本発明の方式によれば高速な光伝送方式にも対応することができる。

【0021】デジタル式であるから、隠蔽化鍵だけを使用すれば済み、復号器側のカオス信号の参照信号はいらないし、情報伝送中のノイズには影響されず、鍵の長短は自由にすることができることで、ユーザはその便利さと安全さのバランスを簡単に取れる。

【0022】本発明の方式では機密保護の対象とする平文の長短は自由であり、英文、日本語、中国語、また、テキスト、バイナリイ、グラフィックなどのどんな種類の平文にも対応できる。

【0023】

【発明の実施の形態】本発明の実施例について説明する。本発明の実施例を図6、図7、図8のダンプリストに示す。そこで、図6の平文に対して、文字列"123"を鍵として入力すれば、図7の隠蔽化信号文になる。復号化するとき、同様な文字列"123"を入力して、同様なシステムを用いて復号化を行えば、図8のように平文に戻る。

【0024】

【発明の効果】本発明の方式は、可変長の鍵によって、

鍵の空間は最低 2^{64} ($=1.8E19$)倍以上に拡大、さらに、複数のカオス関数と、遅れと、カオス関数のパラメータをデジタル式カオス信号ペクトルの決める要素として採用することで、デジタル式カオス信号の発生空間を最低 $m \cdot 2^{16} \cdot 2^{64}$ ($=m \cdot 1.2E24$)倍以上に拡大できる。両者が合計すれば、最低、 $m \cdot 2.2E43$ 倍以上拡大できる。即ち安全強度は $m \cdot 2.2E43$ 倍以上に拡大できる。従って、現在使われている解読手法では、隠蔽化鍵が分らないとカオス隠蔽を解読することが不可能であり、多鍵多重カオスを用いたシステムを採用すれば、解読することは不可能であることからより安全性が高いシステムとなる。

【0025】また、カオス信号の発生は速く、かつ、ストリーミ的な処理であるからことから、高速通信にも対応できる。デジタル式であるから、隠蔽化鍵だけを使用すれば済み、復号器側のカオス信号の参照信号はいらない。まだ、ノイズには影響されない。

【0026】鍵の長短は自由にできることで、ユーザはその便利さと安全さのバランスを簡単に取れる。平文の

長短は自由であり、英文、日本語、中国語、また、テキスト、バイナリ、グラフィックなどのどんな種類の平文にも対応できる。コンピュータ上でソフトウェアだけで処理可能であるし、LSI化することも可能である。信号の高速的な光伝送方式にも対応することができる。

【図面の簡単な説明】

【図1】本発明のカオス隠蔽化方式の概念図である。

【図2】ロジスティック写像カオスの時系列波形である。

【図3】隠蔽化手続きのフロー・ダイアグラムである。

【図4】復号化手続きのフロー・ダイアグラムである。

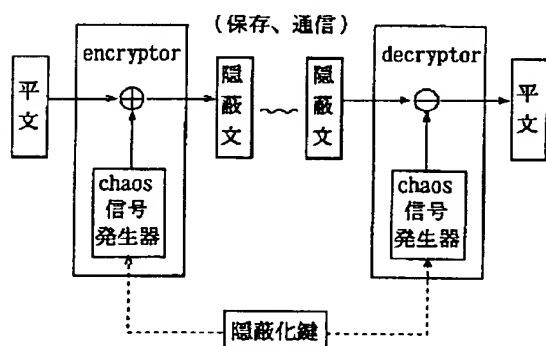
【図5】多鍵多重カオス隠蔽化システムの概念図である。

【図6】平文のサンプルである。

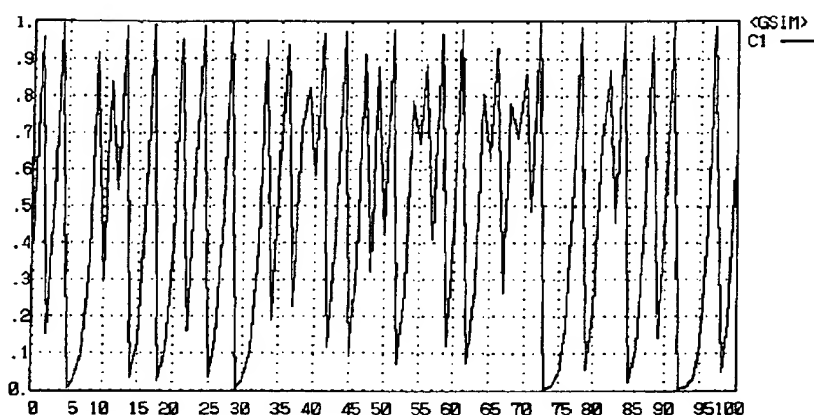
【図7】隠蔽文のサンプルである。

【図8】復号された平文のサンプルである。

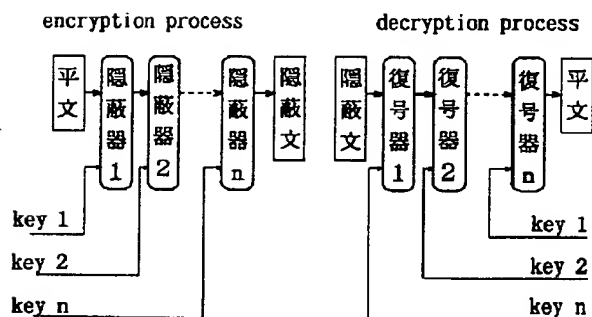
【図1】



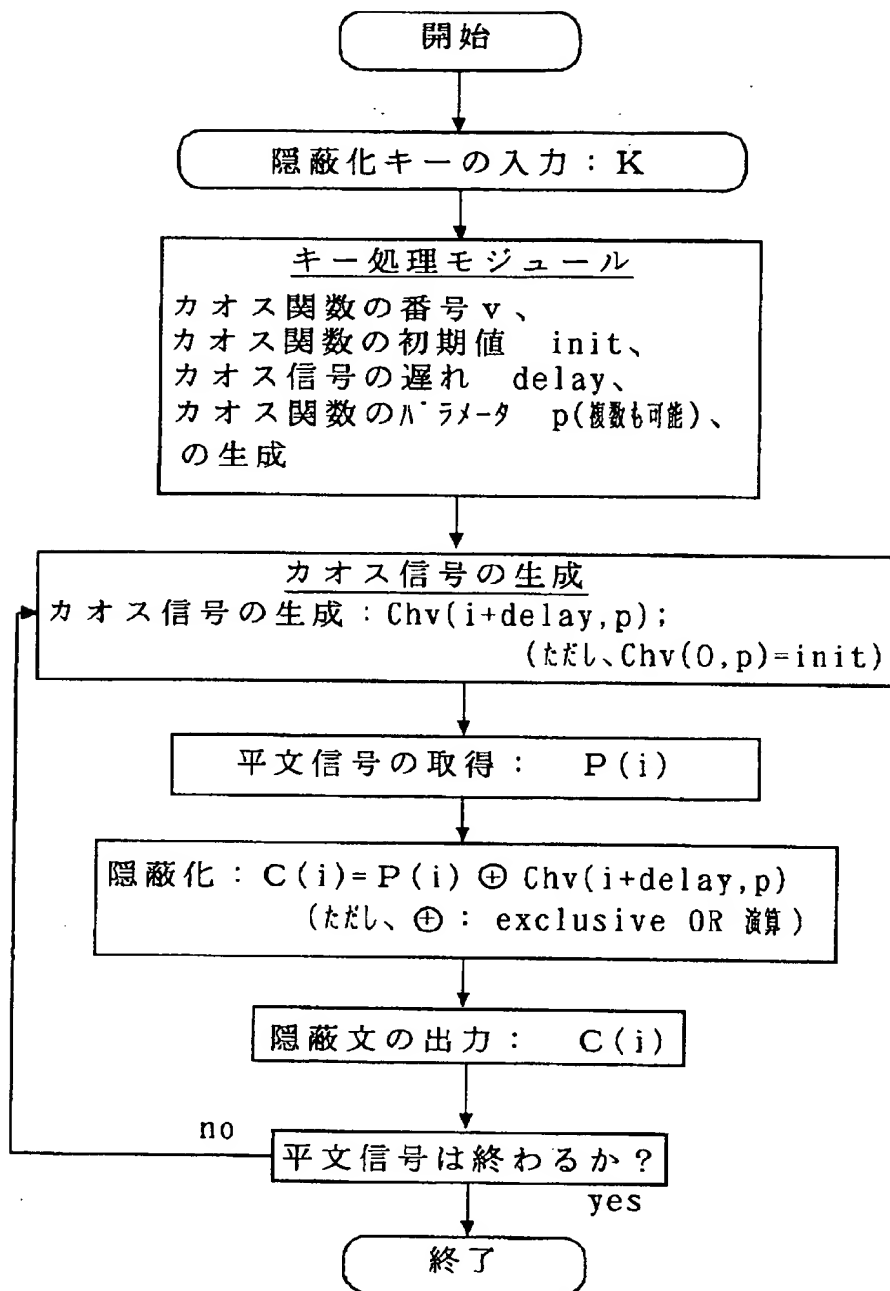
【図2】



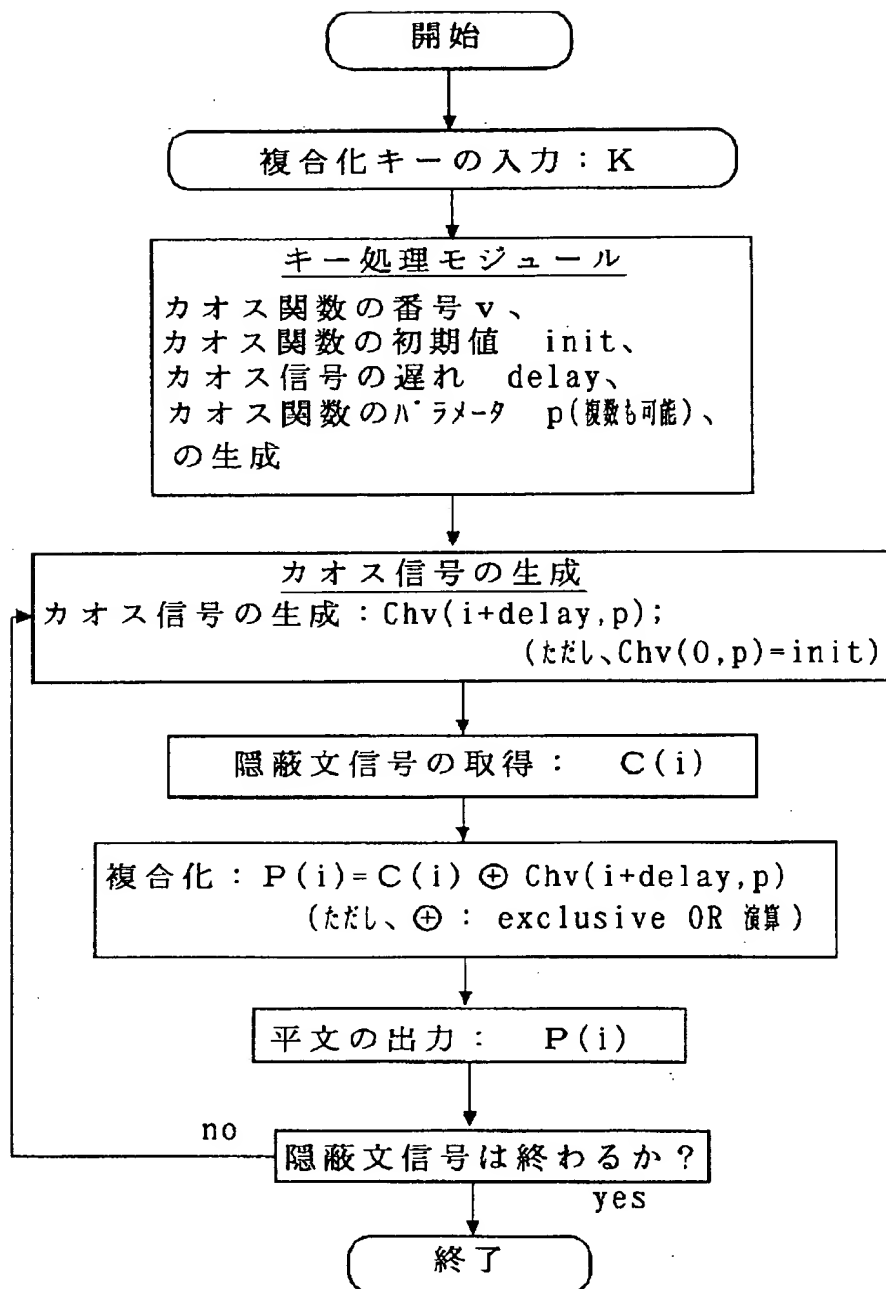
【図5】



【図3】



【図4】



【図 7】

```

00000000 F9 03 64 19 26 E9 63 55-14 00 DF B0 8E F1 B4 65      ...d. ぢぢぢゝダス首xε
00000010 5F 9E FC 05 1C 84 10 E9-00 43 79 69 25 B8 43 03      ... 拾3... Cyf7xKJ
00000020 87 F3 5D 71 87 78 68 83-A2 A7 C8 AB 0A 3A 16 16      ... じDq3 kΔ pti-1j
00000030 4B 57 E8 53 39 AA 28 F3-F7 60 21 EA 2F 43 03 C3      ...K089x+... 1. /CJ
00000040 3A 15 E9 F2 A4 36 9C 68-62 51 2B CA 92 38 30 C0      ... 豈. 6fB0pΔn-8-7
00000050 68 22 06 86 18 69 BE-70 DE 60 85 86 B5 D0 10      ...ah"カじじゝ ぢぢじじ
00000060 74 E2 35 F6 44 B4 B0-A8-60 4A 4A 3A 90 40 45      ...t.5...I-y... ぢぢぢぢE
00000070 03 13 63 B0 1A B6 22 1E-1A CD 71 CA F3 65 92 73      ... ぢ... ぢ... ぢ... ぢ...
00000080 09 91 2A 08 E9 3B 27 99-8B B1 B6 08 7F 30 F8 52      ... ぢ... ぢ... ぢ... ぢ...
00000090 58 FB A0 7F 03 10 31 29-9C E4 75 89 04 89 E4 04      ...X.....1 ぢぢぢ... 我...
000000A0 42 E2 5F 5C 7F C8 F0 44-14 90 18 95 15 D9 03 81      ... ぢヱヱ... ぢぢ...
000000B0 4E 59 82 66 54 B6 08-A7 10 30 4E 70 04 16 AB      ... ぢ... ぢ... ぢ... ぢ...
000000C0 D9 FD 33 87 06 D5 27 9F-36 7B D5 61 D5 A3 12 6C      ... ぢ... 3... 5[ぢぢ... 1
000000D0 43 D3 27 42 B6 52 52 38-87 22 A1 FE AF EC 47 01      ...1E[ぢぢ... ぢ... ぢ...
000000E0 E8 08 5A D0 19 37 03 EF-E9 8E A6 48 3A 68 5E 59      ... ぢ... 7... ぢ... ぢ...
000000F0 59 01 65 C1 FC 6A 70 A0-F8 A8 75 DA 27 95 EE 06      ...Y.ぢ... ぢ... ぢ...
00000100 74 AD 62 CA 2F 15 87 81-34 9F 82 4E 29 34 45 B3      ...tabV... ぢ... ぢ... ぢ...
00000110 CA A6 30 C2 8D C5 27 60-66 29 A9 08 C3 A4 E2 BE      ...1[ぢぢ... ぢ... ぢ...
00000120 81 F1 62 95 58 48 75 68-41 21 66 4E 41 57 82 F0      ... ぢ... ぢ... ぢ... ぢ...
00000130 A6 07 0A 0A D8 23 CD CF-10 B3 A8 74 5F 31 5F 7D      ... ぢ... ぢ... ぢ... ぢ...
00000140 F8 03 65 99 57 79 83 55-64 01 ED 06 E1 B6 71 13      ... ぢ... ぢ... ぢ... ぢ...
00000150 35 30 91 C1 70 8F DE 27-09 97 83 18 08 8F 9A 87      ...50 ぢ... ぢ... ぢ... ぢ...
00000160 93 2C 8F 0D 8F 81 D6 02-18 65 EF 03 3A 3A 70 08      ... ぢ... ぢ... ぢ... ぢ...
00000170 A9 00 A8 33 16 77 BA 55-66 88 2D 29 D0 08 29      ... ぢ... ぢ... ぢ... ぢ...
00000180 8F 56 F3 16 92 CF 5F B0-00 6C 4C 01 08 68 CD 0C      ... ぢ... ぢ... ぢ... ぢ...
00000190 1F 0C 4D E1 B6 2C 65 B4-61 B6 E4 0E A1 69 5D B5      ... ぢ... ぢ... ぢ... ぢ...
000001A0 6C 3D

```

[illegible]